

07.10.2004

日本国特許庁
JAPAN PATENT OFFICE

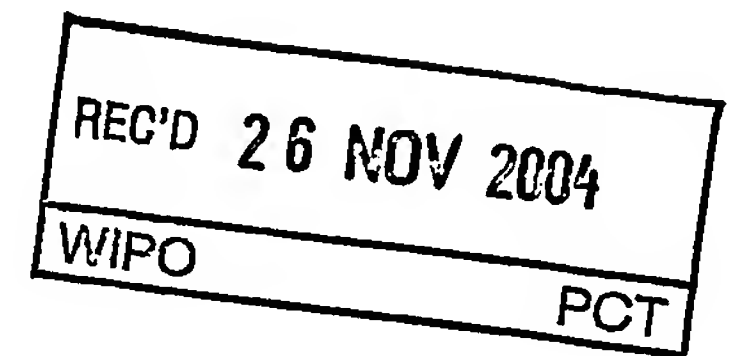
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年10月28日

出願番号
Application Number: 特願2003-367527
[ST. 10/C]: [JP2003-367527]

出願人
Applicant(s): 財団法人生産技術研究奨励会

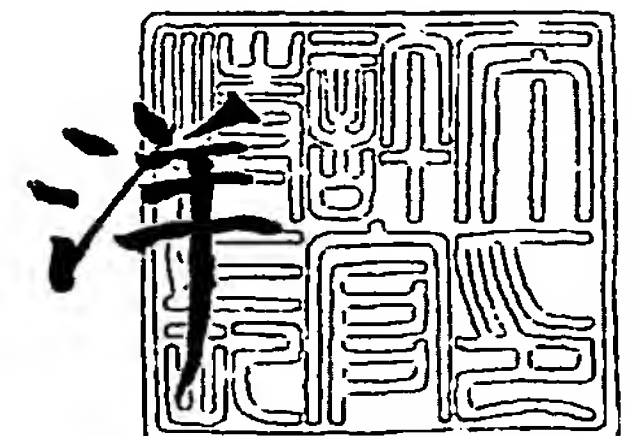


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年11月12日

特許庁長官
Commissioner,
Japan Patent Office

小川



BEST AVAILABLE COPY

出証番号 出証特2004-3102372

【書類名】 特許願
【整理番号】 IIS03014
【提出日】 平成15年10月28日
【あて先】 特許庁長官 殿
【国際特許分類】 B65C 9/00
【発明者】
 【住所又は居所】 神奈川県横浜市戸塚区品濃町 5 5 7 - 4 4 - 2 0 5
 【氏名】 今井 秀樹
【発明者】
 【住所又は居所】 東京都三鷹市大沢 2 - 2 0 - 3 1 - 1 - 4 0 2
 【氏名】 古原 和邦
【発明者】
 【住所又は居所】 東京都目黒区駒場四丁目 6 番 1 号 東京大学生産技術研究所内
 【氏名】 辛 星漢
【特許出願人】
 【識別番号】 801000049
 【氏名又は名称】 財団法人生産技術研究奨励会
【代理人】
 【識別番号】 100064908
 【弁理士】
 【氏名又は名称】 志賀 正武
【選任した代理人】
 【識別番号】 100108578
 【弁理士】
 【氏名又は名称】 高橋 詔男
【選任した代理人】
 【識別番号】 100089037
 【弁理士】
 【氏名又は名称】 渡邊 隆
【選任した代理人】
 【識別番号】 100101465
 【弁理士】
 【氏名又は名称】 青山 正和
【選任した代理人】
 【識別番号】 100094400
 【弁理士】
 【氏名又は名称】 鈴木 三義
【選任した代理人】
 【識別番号】 100107836
 【弁理士】
 【氏名又は名称】 西 和哉
【選任した代理人】
 【識別番号】 100108453
 【弁理士】
 【氏名又は名称】 村山 靖彦
【手数料の表示】
 【予納台帳番号】 008707
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0203645

【書類名】 特許請求の範囲**【請求項 1】**

端末装置とサーバ間において相互に認証を行う認証システムであって、

前記端末装置は、

ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データ H とユーザ保存用の認証情報 P' を求めるデータ伸長手段と、

前記データ伸長手段によって求めた認証情報 P' を予め記憶しておく記憶手段と、

前記記憶手段から読み出した認証情報 P' と認証時に入力されたパスワードを入力として所定の計算式により値 P を求める結合手段と、

前記値 P と内部において発生させた乱数を入力として所定の計算式により値 Y 1 を求め、前記サーバへ送信するマスク演算手段と、

前記値 P と内部において発生させた乱数と前記サーバから受信した値 Y 2 を入力として所定の計算式により値 MK を求めるマスター鍵生成手段と、

前記値 MK を入力として所定の計算式により値 V 1 を求め、サーバへ送信するとともに、前記サーバから受信した値 V 2 と値 V 1 と比較照合し、一致した場合にサーバを認証する認証結果判断手段と

を備え、

前記サーバは、

前記データ伸長手段によって求めたパスワード認証データ H を予め記憶しておく記憶手段と、

前記記憶手段から読み出したパスワード認証データ H と内部において発生させた乱数を入力として所定の計算式により値 Y 2 を求め、前記端末装置へ送信するマスク演算手段と、

前記パスワード認証データ H と内部において発生させた乱数と前記端末装置から受信した値 Y 1 を入力として所定の計算式により値 MK を求めるマスター鍵生成手段と、

前記値 MK を入力として所定の計算式により値 V 2 を求め、端末装置へ送信するとともに、前記端末装置から受信した値 V 1 と値 V 2 と比較照合し、一致した場合に端末装置を認証する認証結果判断手段と

を備えたことを特徴とする認証システム。

【請求項 2】

前記端末装置及びサーバは、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成手段をそれぞれに備えたことを特徴とする請求項 1 に記載の認証システム。

【請求項 3】

前記認証情報 P' は、多項式であることを特徴とする請求項 1 または 2 に記載の認証システム。

【請求項 4】

前記認証情報 P' は、ハッシュ関数であることを特徴とする請求項 1 または 2 に記載の認証システム。

【請求項 5】

前記認証情報 P' は、疑似乱数関数であることを特徴とする請求項 1 または 2 に記載の認証システム。

【請求項 6】

端末装置とサーバ間において相互に認証を行う認証システムにおける端末装置上で動作する認証プログラムであって、

ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データ H とユーザ保存用の認証情報 P' を求めるデータ伸長処理と、

前記データ伸長処理によって求めた認証情報 P' を予め記憶しておく記憶処理と、

前記記憶処理により記憶しておいた認証情報 P' と認証時に入力されたパスワードを入力として所定の計算式により値 P を求める結合処理と、

前記値 P と内部において発生させた乱数を入力として所定の計算式により値 Y 1 を求め、前記サーバへ送信するマスク演算処理と、

前記値 P と内部において発生させた乱数と前記サーバから受信した値 Y 2 を入力として所定の計算式により値 M K を求めるマスター鍵生成処理と、

前記値 M K を入力として所定の計算式により値 V 1 を求め、サーバへ送信するとともに、前記サーバから受信した値 V 2 と値 V 1 と比較照合し、一致した場合にサーバを認証する認証結果判断処理と

をコンピュータに行わせることを特徴とする認証プログラム。

【請求項 7】

相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする請求項 6 に記載の認証プログラム。

【請求項 8】

端末装置とサーバ間において相互に認証を行う認証システムにおけるサーバ上で動作する認証プログラムであって、

パスワード認証データ H を予め記憶しておく記憶処理と、

前記記憶処理により記憶しておいたパスワード認証データ H と内部において発生させた乱数を入力として所定の計算式により値 Y 2 を求め、前記端末装置へ送信するマスク演算処理と、

前記パスワード認証データ H と内部において発生させた乱数と前記端末装置から受信した値 Y 1 を入力として所定の計算式により値 M K を求めるマスター鍵生成処理と、

前記値 M K を入力として所定の計算式により値 V 2 を求め、端末装置へ送信するとともに、前記端末装置から受信した値 V 1 と値 V 2 と比較照合し、一致した場合に端末装置を認証する認証結果判断処理と

をコンピュータに行わせることを特徴とする認証プログラム。

【請求項 9】

相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする請求項 8 に記載の認証プログラム。

【請求項 10】

前記認証情報 P' は、多項式であることを特徴とする請求項 6 ないし 9 のいずれかに記載の認証プログラム。

【請求項 11】

前記認証情報 P' は、ハッシュ関数であることを特徴とする請求項 6 ないし 9 のいずれかに記載の認証プログラム。

【請求項 12】

前記認証情報 P' は、疑似乱数関数であることを特徴とする請求項 6 ないし 9 のいずれかに記載の認証プログラム。

【書類名】 明細書

【発明の名称】 認証システム

【技術分野】

【0001】

本発明は、認証に関する情報の漏洩に強い認証システムに関する。

【背景技術】

【0002】

従来からユーザの端末装置とサーバとの間において認証を行う方法として、ユーザIDとユーザのみが知っているパスワードとを端末装置から入力し、サーバ側に蓄えられている情報と一致すれば、正当なユーザであることを認証する方法が知られている。

しかし、この方法は、端末装置とサーバ間の通信経路中において、不正にこれらの情報が盗まれてしまうと、簡単に不正利用を許してしまうため、SSL（非特許文献1）、TLS（非特許文献2）、SSH（非特許文献3）等の暗号化技術を用いて、情報の送受信を行うのが一般的である。これは、パスワードと秘密の値と公開されている値とを使用し、て認証を行うものである。

【非特許文献1】 A.Frier, P.Karlton, and P.Kocher. The SSL 3.0 Protocol. Netscape Communications Corp., 1996, <http://wp.netcape.com/eng/ssl3/>

【非特許文献2】 IETF(Internet Engineering Task Force). Transport Layer security (tls) Charter. <http://www.ietf.org/html.charters/tls-charter.html>

【非特許文献3】 IETF(Internet Engineering Task Force). Secure Shell(secsh) Charter. <http://www.ietf.org/html.charters/secsh-charter.html>

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかしながら、非特許文献1～3に示す方法は、ユーザ側から暗号化された情報が漏れた場合は、オフラインの解析作業によってパスワードを求めることができってしまうという問題がある。サーバに対してオンラインでパスワード入力を繰り返し行う方法は、パスワードを間違えた回数に応じてアクセスを拒否するなどの対策を講じることが可能であるが、オフラインの解析作業は、防止策を講じることができないという問題もある。

【0004】

本発明は、このような事情に鑑みてなされたもので、情報の漏洩に強く、安全に暗号鍵の交換を行うことができる認証システムを提供することを目的とする。

【課題を解決するための手段】

【0005】

請求項1に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムであって、前記端末装置は、ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データHとユーザ保存用の認証情報P'を求めるデータ伸長手段と、前記データ伸長手段によって求めた認証情報P'を予め記憶しておく記憶手段と、前記記憶手段から読み出した認証情報P'と認証時に入力されたパスワードを入力として所定の計算式により値Pを求める結合手段と、前記値Pと内部において発生させた乱数を入力として所定の計算式により値Y1を求め、前記サーバへ送信するマスク演算手段と、前記値Pと内部において発生させた乱数と前記サーバから受信した値Y2を入力として所定の計算式により値MKを求めるマスター鍵生成手段と、前記値MKを入力として所定の計算式により値V1を求め、サーバへ送信するとともに、前記サーバから受信した値V2と値V1と比較照合し、一致した場合にサーバを認証する認証結果判断手段とを備え、前記サーバは、前記データ伸長手段によって求めたパスワード認証データHを予め記憶しておく記憶手段と、前記記憶手段から読み出したパスワード認証データHと内部において発生させた乱数を入力として所定の計算式により値Y2を求め、前記端末装置へ送信するマスク演算手段と、前記パスワード認証データHと内部において発生させた乱数と前記端末装置から受信した値Y1を入力として所定の計算式により値MKを求めるマスター鍵生成手

段と、前記値MKを入力として所定の計算式により値V2を求め、端末装置へ送信するとともに、前記端末装置から受信した値V1と値V2と比較照合し、一致した場合に端末装置を認証する認証結果判断手段とを備えたことを特徴とする。

【0006】

請求項2に記載の発明は、前記端末装置及びサーバは、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成手段をそれぞれに備えたことを特徴とする。

【0007】

請求項3に記載の発明は、前記認証情報P'は、多項式であることを特徴とする。

【0008】

請求項4に記載の発明は、前記認証情報P'は、ハッシュ関数であることを特徴とする。

【0009】

請求項5に記載の発明は、前記認証情報P'は、疑似乱数関数であることを特徴とする。

【0010】

請求項6に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムにおける端末装置上で動作する認証プログラムであって、ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データHとユーザ保存用の認証情報P'を求めるデータ伸長処理と、前記データ伸長処理によって求めた認証情報P'を予め記憶しておく記憶処理と、前記記憶処理により記憶しておいた認証情報P'と認証時に入力されたパスワードを入力として所定の計算式により値Pを求める結合処理と、前記値Pと内部において発生させた乱数を入力として所定の計算式により値Y1を求め、前記サーバへ送信するマスク演算処理と、前記値Pと内部において発生させた乱数と前記サーバから受信した値Y2を入力として所定の計算式により値MKを求めるマスター鍵生成処理と、前記値MKを入力として所定の計算式により値V1を求め、サーバへ送信するとともに、前記サーバから受信した値V2と値V1と比較照合し、一致した場合にサーバを認証する認証結果判断処理とをコンピュータに行わせることを特徴とする。

【0011】

請求項7に記載の発明は、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする。

【0012】

請求項8に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムにおけるサーバ上で動作する認証プログラムであって、パスワード認証データHを予め記憶しておく記憶処理と、前記記憶処理により記憶しておいたパスワード認証データHと内部において発生させた乱数を入力として所定の計算式により値Y2を求め、前記端末装置へ送信するマスク演算処理と、前記パスワード認証データHと内部において発生させた乱数と前記端末装置から受信した値Y1を入力として所定の計算式により値MKを求めるマスター鍵生成処理と、前記値MKを入力として所定の計算式により値V2を求め、端末装置へ送信するとともに、前記端末装置から受信した値V1と値V2と比較照合し、一致した場合に端末装置を認証する認証結果判断処理とをコンピュータに行わせることを特徴とする。

【0013】

請求項9に記載の発明は、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする。

【0014】

請求項10に記載の発明は、前記認証情報P'は、多項式であることを特徴とする。

【0015】

請求項11に記載の発明は、前記認証情報P'は、ハッシュ関数であることを特徴とする。

【0016】

請求項 12 に記載の発明は、前記認証情報 P' は、疑似乱数関数であることを特徴とする。

【発明の効果】

【0017】

この発明によれば、端末装置側あるいはサーバ側から装置内に保存している情報が漏れたとしてもオフライン解析によってパスワードを見つけだすことができないため、サーバの不正利用を防止することが可能になるという効果が得られる。また、装置内に保存されている情報を盗まれないようにするための耐タンパー性のモジュールを使用する必要がないため、装置構成を簡単にすることができる。また、公開鍵暗号システムのように複雑な鍵管理処理を行う必要がないため、計算処理を向上させることができるとともに、処理内容を簡単にすることができる。

【発明を実施するための最良の形態】

【0018】

以下、本発明の一実施形態による認証システムを図面を参照して説明する。この認証システムは、ユーザの端末装置とサーバの認証装置がお互いに相互認証しながら同じセッション鍵を確保するためのシステムである。

ここで、以下の説明において用いる記号について説明しておく。

p , q は素数であり、 $q \mid p-1$ という関係がある。また、 g , h は $\text{mod } p$ 上の位数 q の有限体(群) G の生成元である (楕円曲線上の群でも同じように構成できる)。ここで、 g は $(1 < g < p-1, g^q = 1 \text{ mod } p)$ であり、 h は $h = g^a \text{ mod } p$ である。つまり、 p , q は演算体系を示す。例えば、 $H = h^x \text{ mod } p$ ($0 \leq x < q$) で x は秘密情報である ($x = \log_h H$; H の生成元 h に対する離散対数)。また、乱数発生器から発生される乱数は $R \in \mathbb{Z}/q\mathbb{Z}$ を無作為に生成する。

【0019】

<端末装置初期化>

ユーザは、サーバに対して個人登録したい時、自分の端末装置の初期化を行う。図 1 は、ユーザの端末装置の初期化処理の構成を示すブロック図である。初期化は、ユーザがパスワードを入力すると、データ伸張器 11 によって、サーバ登録用のパスワード認証データ H と、ユーザ保存用の値 P' が生成され、パスワード認証データ H は、サーバに受け渡され、値 P' は、メモリ 12 へ保存する。ここで、データ伸張器 11 は、(1) 多項式、(2) ハッシュ関数、(3) 疑似乱数発生器などで構成することが可能である。

【0020】

(1) 多項式を利用する場合

初めに、図 2 を参照して、多項式を利用する場合について説明する。

まず、多項式発生器 111 によりランダムに多項式を発生する。このとき、登録するサーバの数が一つだったら 1 次多項式を n だったら n 次多項式を発生する。例えば、一つのサーバの場合、 $p'(x)$ は、 $p'(x) = a_1 \cdot x \text{ mod } q$ となる。ここで、ユーザは自分が覚えているパスワード (例えば、"P o o h 9 3") を入力する。多項式とユーザのパスワードが入力されたらパスワード認証データ生成器 112 は、パスワード認証データ H を生成する。パスワード認証データ H は、例えば $H = h^{p'(1)} + \text{P o o h 9 3} \text{ mod } p$ により計算できる。ここで、 $p'(1)$ は $p'(x)$ で x の代わりにサーバの ID (例えば、「1」) 入れて計算した値である。パスワード認証データ H はユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ 12 は多項式発生器から発生された多項式 $P' = p'(x)$ を記憶して保存する。

【0021】

(2) ハッシュ関数を利用する場合

次に、図 3 を参照して、ハッシュ関数を利用する場合について説明する。

まず、ハッシュ関数発生器 113 によりランダムにハッシュ関数 $HASH$ を発生する。そして、秘密値発生器 114 もランダムに秘密値 S を発生する。ここで、ユーザは自分が

覚えているパスワード（例えば、“P o o h 9 3”）を入力する。ハッシュ関数HASHと秘密値Sとユーザのパスワードが入力されたらパスワード認証データ生成器115はパスワード認証データHを生成する。Hは、 $H = h^{HASH}(S \parallel P o o h 9 3 \parallel 1) \bmod p$ により計算できる。ここで、「1」はサーバのIDを表す。パスワード認証データHはユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ12はハッシュ関数発生器113と秘密値発生器114から発生されたハッシュ関数HASHと秘密値Sと一緒に $P' = (HASH, S)$ として記憶して保存する。

【0022】

(3) 擬似乱数発生器を利用する場合

次に、図4を参照して、擬似乱数発生器を利用する場合について説明する。

まず、擬似乱数発生器116によりランダムに擬似乱数関数PRNGを発生する。そして、秘密値発生器117もランダムに秘密値Sを発生する。ここで、ユーザは自分が覚えているパスワード（例えば、“P o o h 9 3”）を入力する。擬似乱数関数PRNGと秘密値Sとユーザのパスワードが入力されたのを受けて、パスワード認証データ生成器118はパスワード認証データHを生成する。Hは、 $H = h^{PRNG}(S \parallel P o o h 9 3 \parallel 1) \bmod p$ により計算できる。ここで、「1」はサーバのIDを表す。パスワード認証データHはユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ12は擬似乱数発生器116と秘密値発生器117から発生させた擬似乱数関数PRNGと秘密値Sと一緒に $P' = (PRNG, S)$ として記憶して保存する。

【0023】

次に、図6、7を参照して、前述した初期化を行った端末装置1とサーバ2（図5参照）との間で相互認証及び鍵交換を行う動作を説明する。

【0024】

<端末装置の動作>

(1) 多項式を利用した場合

初めに、多項式を利用した場合の端末装置1の動作を説明する。

まず、ユーザの端末装置1に備えたメモリ12から記憶された多項式 $P' = p'(x)$ を読み出す。結合器32はメモリ12から読み出した多項式 P' とユーザが入力したパスワードにより $P = p(x)$ を計算して出力する。例えば、 $p(x) = p'(x) + P o o h 9 3 = \alpha_1 \cdot x + P o o h 9 3 \bmod q$ により計算する。マスク演算器34は、結合器32から入力されたPと乱数発生器33において発生させた乱数 R_1 とから Y_1 を、 $Y_1 = g^{R_1} \cdot h^{-P(1)} \bmod p$ により計算する。ここで $p(1)$ は、 $p(1) = p'(1) + P o o h 9 3 = \alpha_1 \cdot 1 + P o o h 9 3 \bmod q$ により計算する。ここで、「1」はサーバの認証IDを表す。通信処理部35は Y_1 をサーバ2へ送信し、サーバ2から Y_2 を受信する。マスター鍵生成器36は結合器32から出力されるPと乱数発生器33から出力される R_1 と受信した Y_2 を入力としてMKを、 $MK = (Y_2 \cdot h^{-P(1)})^{R_1} \bmod p$ により計算して出力する。

【0025】

続いて認証結果判断部37は、MKを入力として、 $V_1 = HASH(00 \parallel Y_1 \parallel Y_2 \parallel MK)$ により V_1 を計算してこの V_1 を通信処理部35によりサーバ2へ送信し、サーバ2から受信した V_2 と V_1 を比較する。ここで、HASHは一方向ハッシュ関数である。

【0026】

次に、認証結果判断部37において V_2 と V_1 が一致しない場合、認証結果判断部37は、エラー発生器38に対して、一致しないことを通知する。これを受けて、エラー発生器38はエラーを発生して処理を中断する。一方、認証結果判断部37において V_2 と V_1 が一致した場合はサーバ2が正当な装置として認証してセッション鍵生成器39は、 $SK = HASH(11 \parallel Y_1 \parallel Y_2 \parallel MK)$ によりセッション鍵SKを生成する。

【0027】

(2) ハッシュ関数を利用した場合

次に、ハッシュ関数を利用した場合の端末装置 1 の動作を説明する。

まず、ユーザの端末装置 1 に備えたメモリ 12 から記憶された P' (HASH, S) を読み出す。ここで、HASH はハッシュ関数、S は秘密値である。結合器 32 はメモリ 12 から読み出した P' とユーザが入力したパスワードにより $P = p(x)$ を計算して出力する。例えば、 $p(x) = \text{HASH}(S \parallel \text{P o o h 9 3} \parallel x) \bmod q$ により計算する。マスク演算器 34 は、結合器 32 から入力された P と乱数発生器 33 において発生させた乱数 R_1 とから Y_1 を、 $Y_1 = g^{R_1} \cdot h^{-P^{(1)}} \bmod q$ により計算する。ここで、 $p^{(1)}$ は、 $p^{(1)} = \text{HASH}(S \parallel \text{P o o h 9 3} \parallel 1) \bmod q$ により計算する。ここで、「1」はサーバの ID を表す。通信処理部 35 は、 Y_1 をサーバ 2 へ送信し、サーバ 2 から Y_2 を受信する。マスター鍵生成器 36 は結合器 32 から出力される P と乱数発生器 33 から出力される R_1 と受信した Y_2 を入力として MK を、 $MK = (Y_2 \cdot h^{-P^{(1)}})^{R_1} \bmod p$ により計算して出力する。

【0028】

続いて認証結果判断部 37 は、 MK を入力として、 $V_1 = \text{HASH}(00 \parallel Y_1 \parallel Y_2 \parallel MK)$ により V_1 を計算してこの V_1 を通信処理部 35 によりサーバ 2 へ送信し、サーバ 2 から受信した V_2 と V_1 を比較する。ここで、HASH は一方向ハッシュ関数である。

【0029】

次に、認証結果判断部 37 において V_2 と V_1 が一致しない場合、認証結果判断部 37 は、エラー発生器 38 に対して、一致しないことを通知する。これを受けて、エラー発生器 38 はエラーを発生して処理を中断する。一方、認証結果判断部 37 において V_2 と V_1 が一致した場合はサーバ 2 が正当な装置として認証してセッション鍵生成器 39 は、 $SK = \text{HASH}(11 \parallel Y_1 \parallel Y_2 \parallel MK)$ によりセッション鍵 SK を生成する。

【0030】

(3) 擬似乱数発生器を利用した場合

次に、擬似乱数関数を利用した場合の端末装置 1 の動作を説明する。

擬似乱数関数を利用した場合は、メモリ 12 に記憶されたハッシュ関数 HASH の代わりに擬似乱数関数 PRNG を用いる以外は、ハッシュ関数を利用した場合と同様の動作であるため、ここでは詳細な説明を省略する。

【0031】

<サーバの動作>

サーバ 2 は、前述した多項式利用した場合、ハッシュ関数利用した場合、擬似乱数利用した場合に関わらず次のように動作する。

サーバ 2 に備えたメモリ 41 に保存されたユーザ ID とパスワードの認証データ H を読み出す。マスク演算器 43 はメモリ 41 から読み出した H と乱数発生器 42 から発生させた乱数 R_2 を入力として Y_2 を、 $Y_2 = g^{R_2} \cdot H = g^{R_2} \cdot h^{P^{(1)}} \bmod p$ により計算する。通信処理部 44 は、計算して得られた Y_2 を端末装置 1 に送信し、端末装置 1 から受信した Y_1 をマスター鍵生成器 45 へ出力する。マスク鍵生成器 45 はメモリ 41 から読み出した H と乱数発生器 42 からの R_2 と通信処理部 44 からの Y_1 を入力として MK を、 $MK = (Y_1 \cdot h^{P^{(1)}})^{R_2} \bmod p$ により計算して、 MK を出力する。

【0032】

続いて認証結果判断部 46 は、 MK を入力として、 $V_2 = \text{HASH}(00 \parallel Y_1 \parallel Y_2 \parallel MK)$ により V_2 を計算してこの V_2 を通信処理部 44 により端末装置 1 へ送信し、端末装置 1 から受信した V_1 と V_2 を比較する。ここで、HASH は一方向ハッシュ関数である。

【0033】

次に、認証結果判断部 46 において V_1 と V_2 が一致しない場合、認証結果判断部 46 は、エラー発生器 47 に対して、一致しないことを通知する。これを受けて、エラー発生器 47 はエラーを発生して処理を中断する。一方、認証結果判断部 46 において V_1 と V_2 が一致した場合は端末装置 1 が正当な装置として認証してセッション鍵生成器 48 は、

$SK = \text{HASH}(11 \parallel Y_1 \parallel Y_2 \parallel MK)$ によりセッション鍵SKを生成する。

【0034】

このように、多項式を利用することにより、不正利用しようとしている者が他人の端末装置を持っていたとしてもユーザのパスワードは情報理論的に安全である。また、サーバ内に侵入して保存されている情報を得たとしてもユーザのパスワードは情報理論的に安全である。また、ハッシュ関数と擬似乱数発生器を利用する場合には、不正利用しようとしている者にとってユーザのパスワードは計算量的に安全である。

【0035】

なお、図1における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより認証処理、鍵交換処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、ホームページ提供環境（あるいは表示環境）を備えたWWWシステムも含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（RAM）のように、一定時間プログラムを保持しているものも含むものとする。

【0036】

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

【図面の簡単な説明】

【0037】

【図1】本発明の一実施形態における端末装置の構成を示すブロック図である。

【図2】図1に示すデータ伸長器11の構成を示すブロック図である。

【図3】図1に示すデータ伸長器11の構成を示すブロック図である。

【図4】図1に示すデータ伸長器11の構成を示すブロック図である。

【図5】相互認証及び鍵交換を行う装置の構成を示すブロック図である。

【図6】図5に示す端末装置1の構成を示すブロック図である。

【図7】図5に示すサーバ2の構成を示すブロック図である。

【符号の説明】

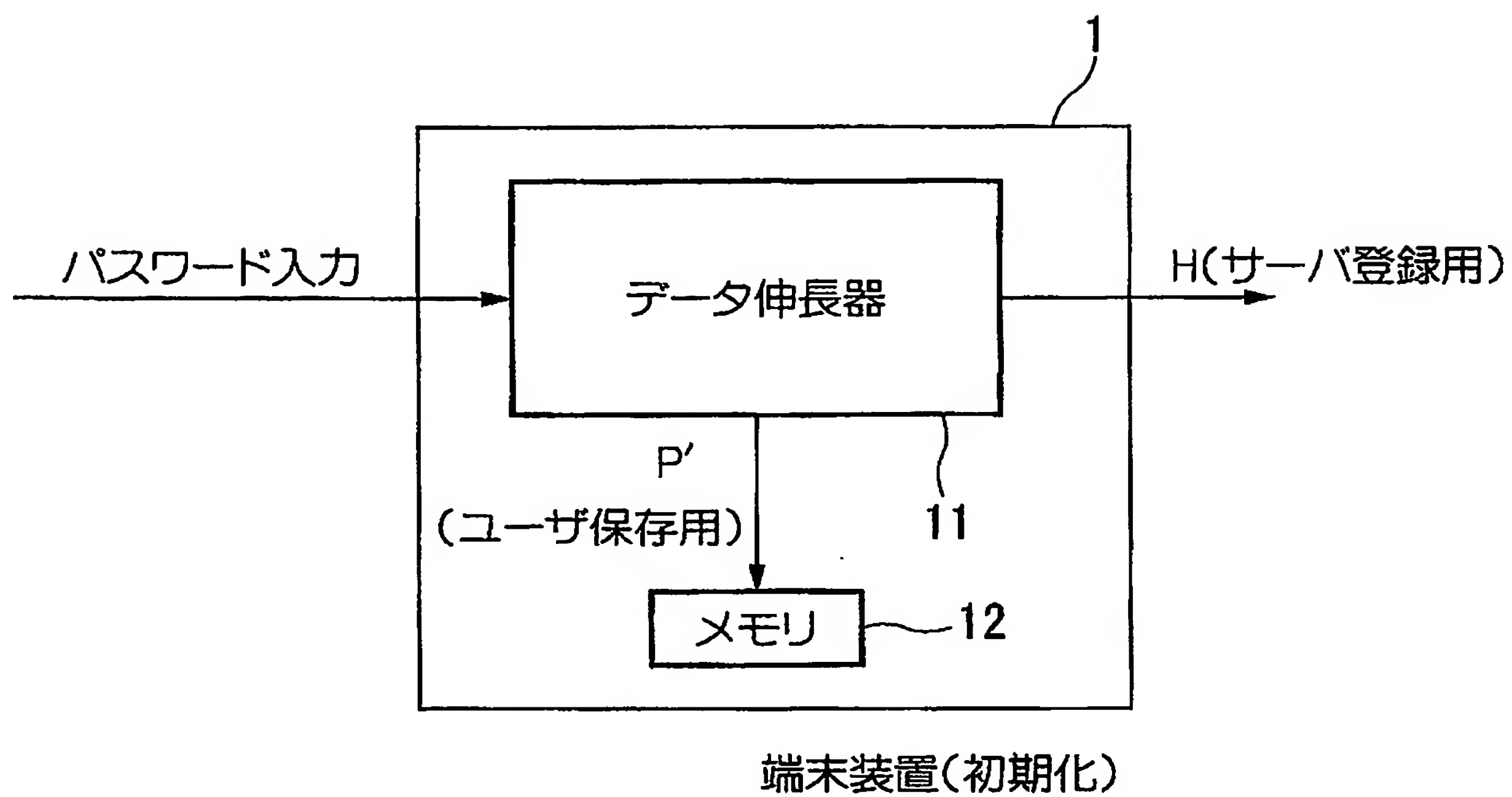
【0038】

- | | |
|----------------------|----------------------|
| 1・・・端末装置、 | 11・・・データ伸長器、 |
| 111・・・多項式発生器、 | 112・・・パスワード認証データ生成器、 |
| 113・・・ハッシュ関数発生器、 | 114・・・秘密値発生器、 |
| 115・・・パスワード認証データ生成器、 | 116・・・擬似乱数発生器、 |
| 117・・・秘密値発生器、 | 118・・・パスワード認証データ生成器、 |
| 12・・・メモリ、 | 32・・・結合器、 |
| 33・・・乱数発生器、 | 34・・・マスク演算器、 |
| 35・・・通信処理部、 | 36・・・マスター鍵生成器、 |
| 37・・・認証結果判断部、 | 38・・・エラー発生器、 |
| 39・・・セッション鍵生成器、 | 2・・・サーバ、 |

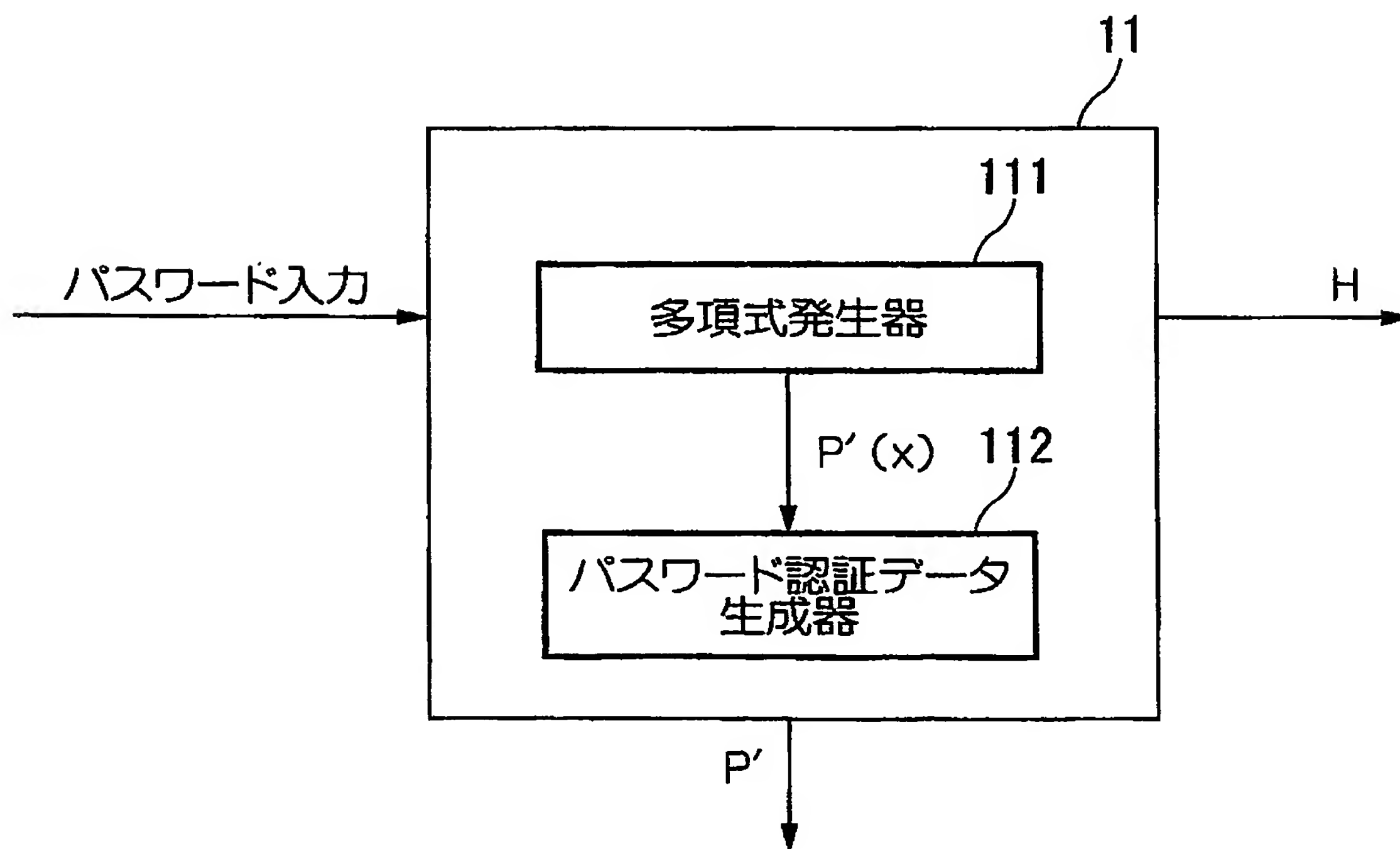
4 1 . . . メモリ、
4 3 . . . マスク演算器、
4 5 . . . マスター鍵生成器、
4 7 . . . エラー発生器、

4 2 . . . 乱数発生器、
4 4 . . . 通信処理部、
4 6 . . . 認証結果判断部、
4 8 . . . セッション鍵生成器

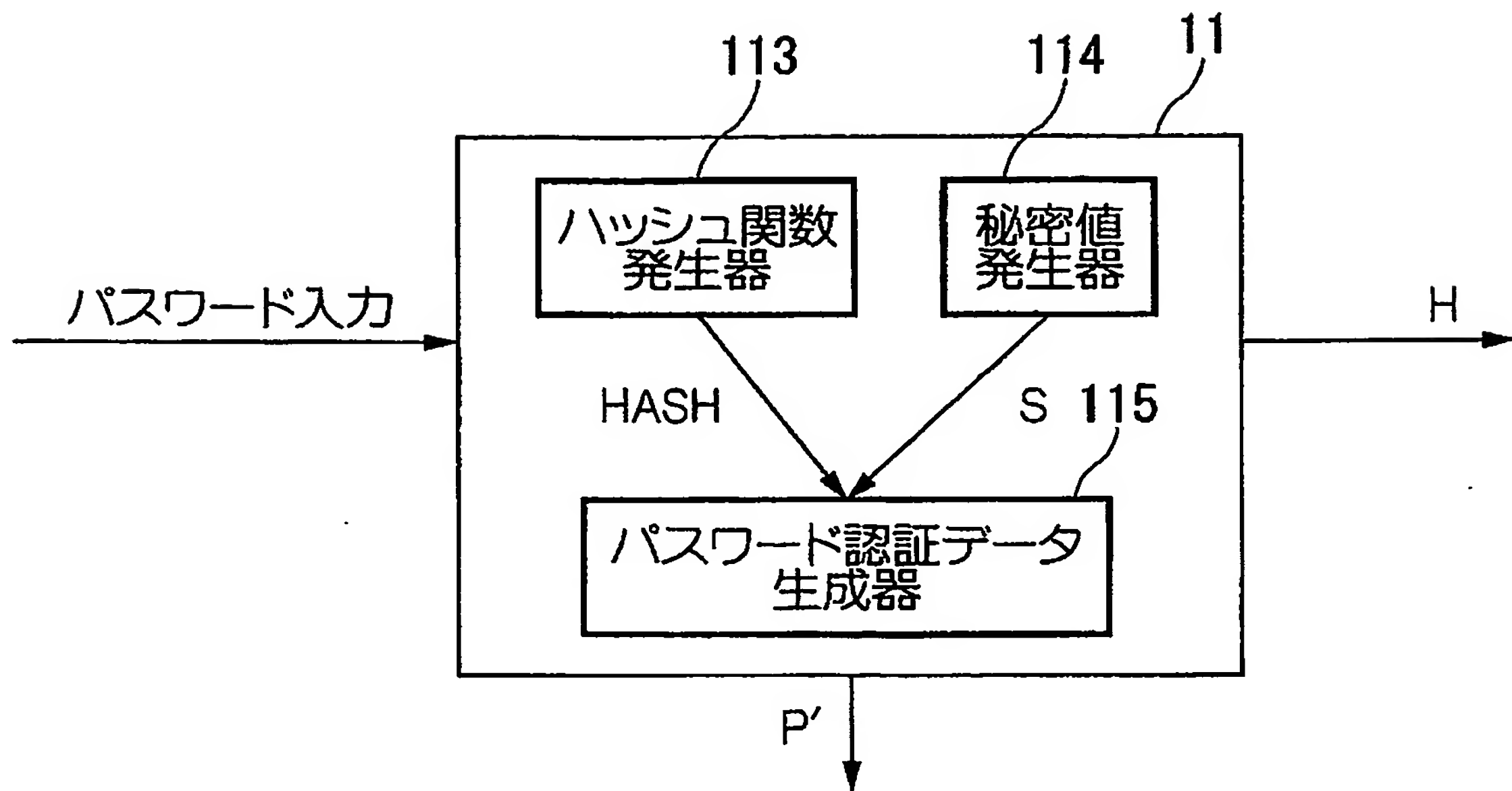
【書類名】 図面
【図 1】



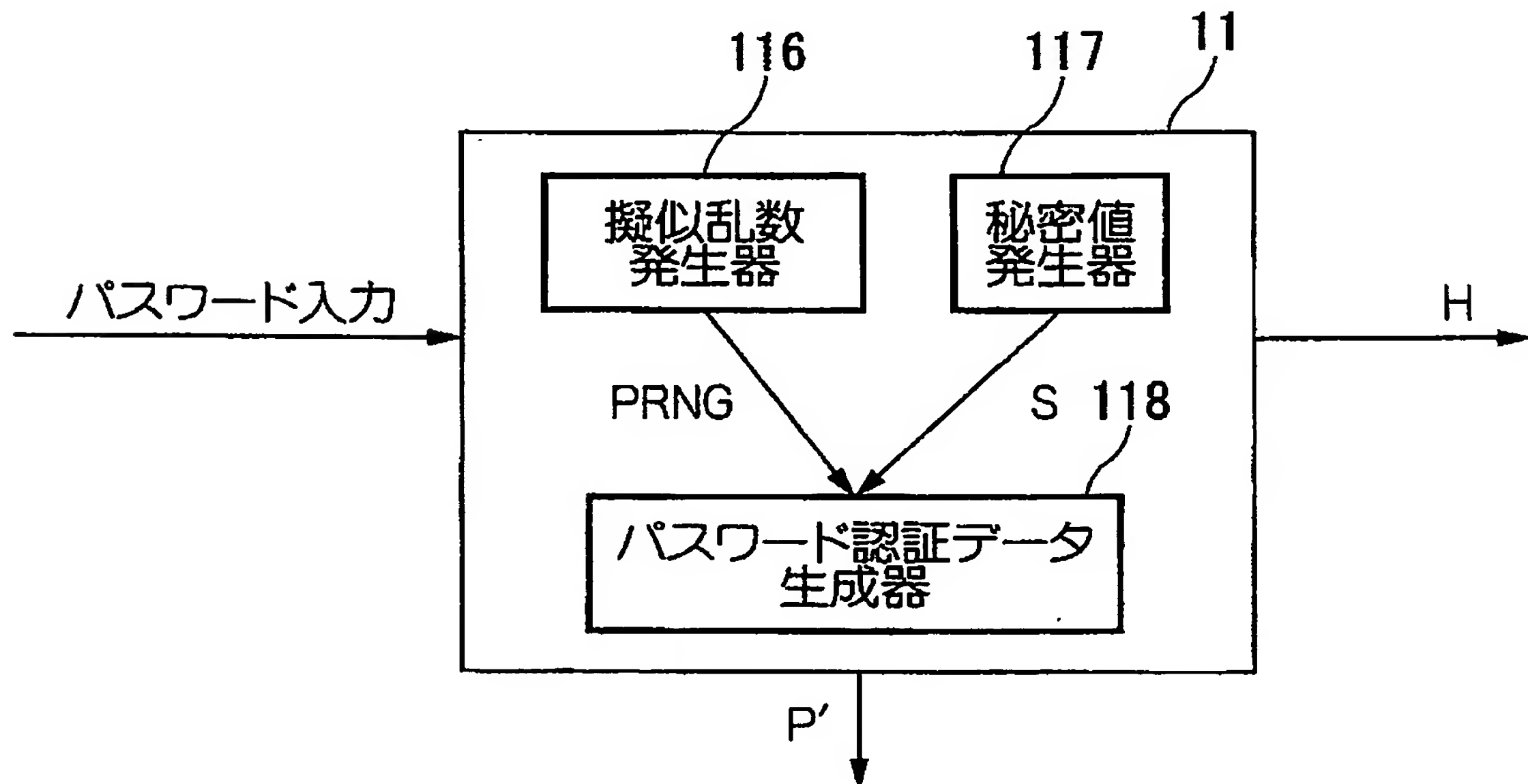
【図 2】



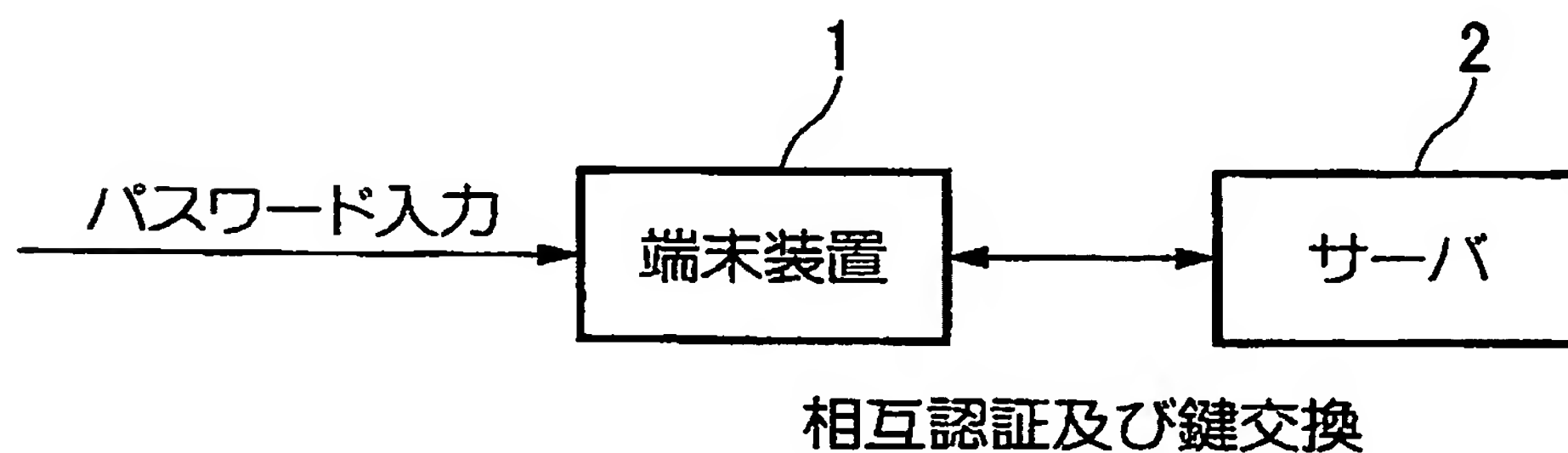
【図 3】



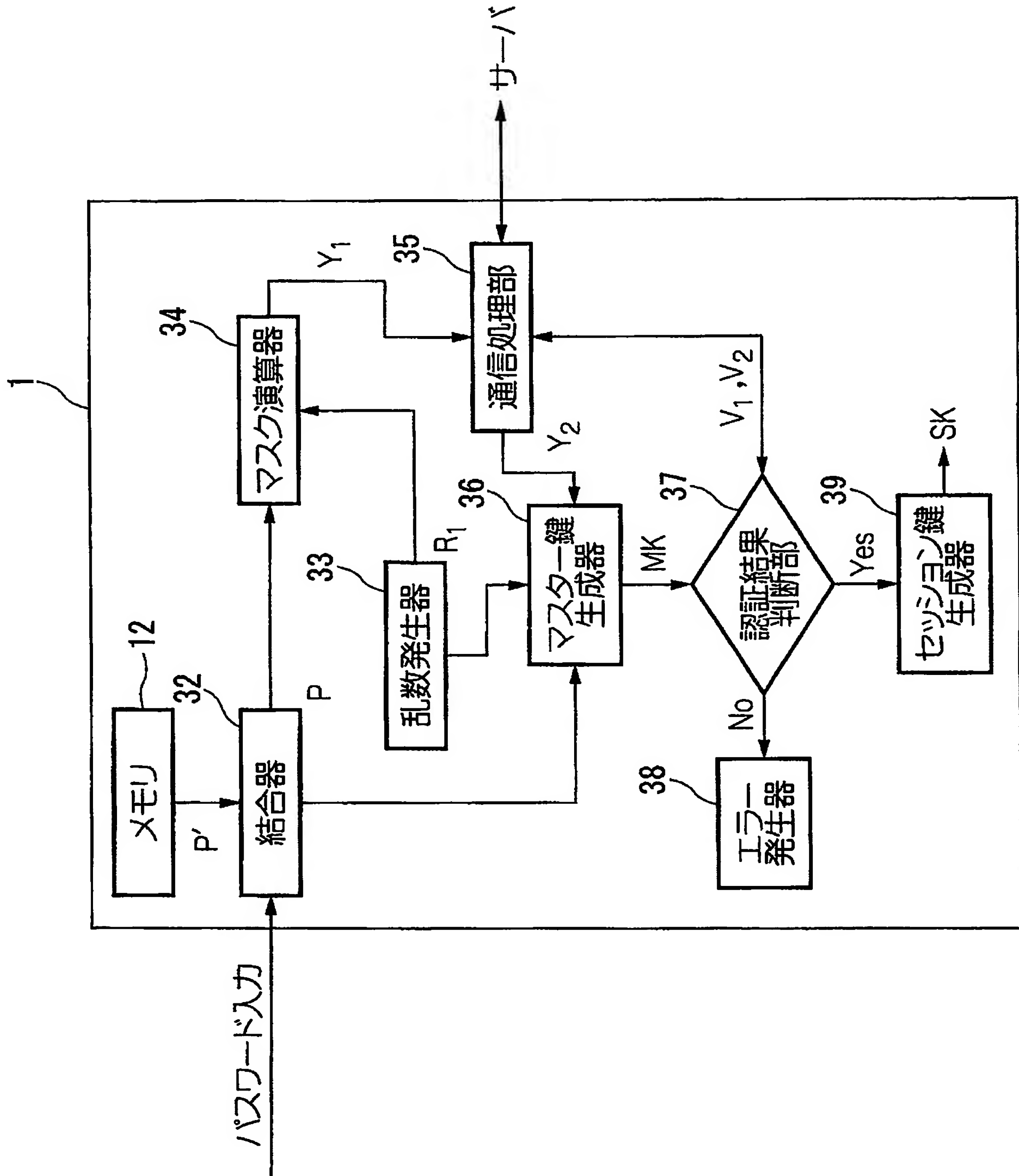
【図 4】



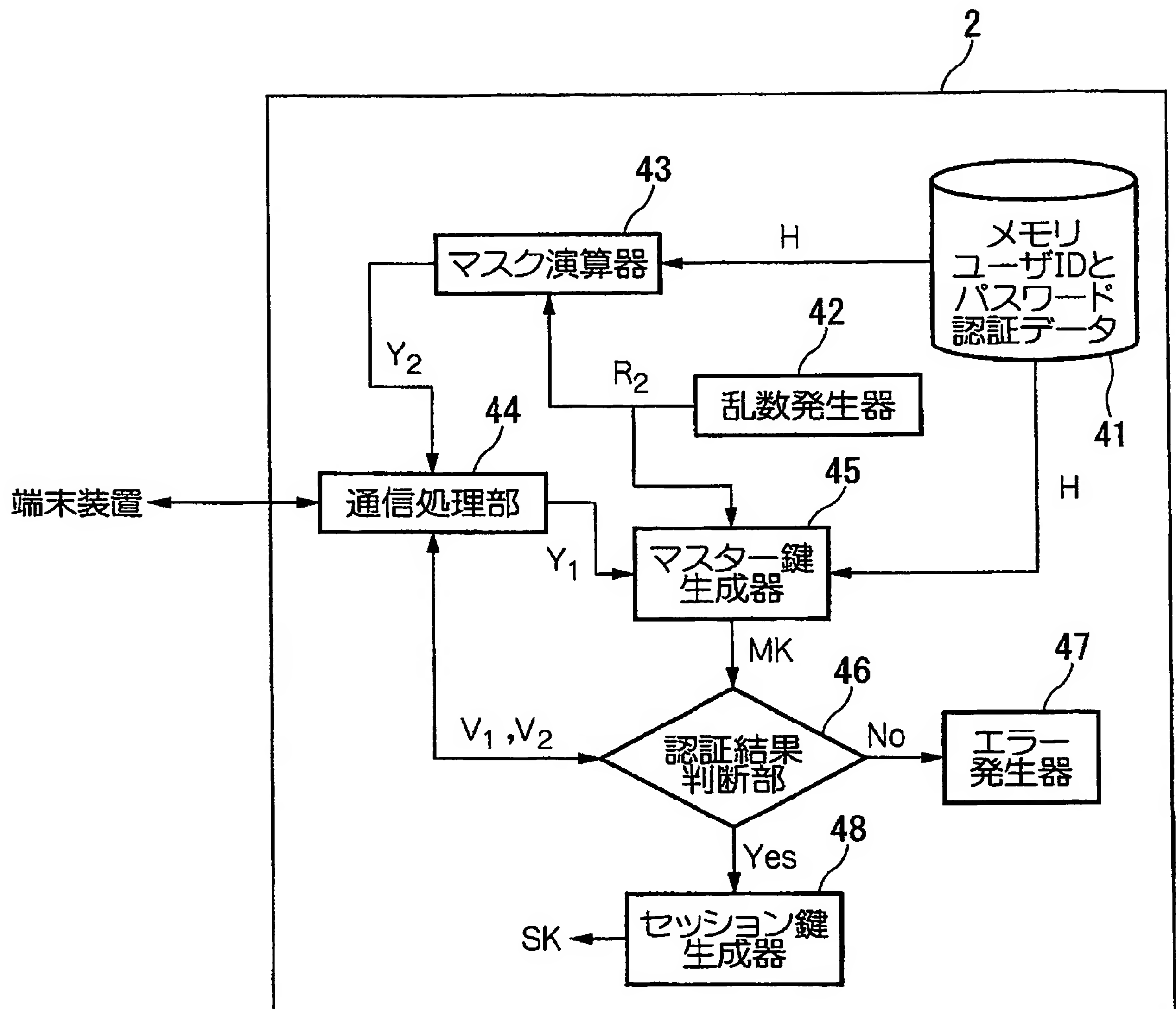
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 情報の漏洩に強く、安全に暗号鍵の交換を行うことができる認証システムを提供する。

【解決手段】 端末装置とサーバ間において相互に認証を行う認証システムであって、ユーザのパスワードに基づいて、パスワード認証データ H と認証情報 P' を求める処理と、求めた認証情報 P' を予め記憶しておく処理と、記憶しておいた認証情報 P' と認証時に入力されたパスワードを入力として所定の計算式により値 P を求める処理と、値 P と内部において発生させた乱数を入力として所定の計算式により値 Y 1 を求め、サーバへ送信する処理と、値 P と内部において発生させた乱数とサーバから受信した値 Y 2 を入力として所定の計算式により値 MK を求める処理と、値 MK を入力として所定の計算式により値 V 1 を求め、サーバへ送信するとともに、サーバから受信した値 V 2 と値 V 1 と比較照合し、一致した場合にサーバを認証する処理とを有する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-367527
受付番号	50301786466
書類名	特許願
担当官	小池 光憲 6999
作成日	平成15年10月30日

<認定情報・付加情報>

【特許出願人】

【識別番号】	801000049
【住所又は居所】	東京都目黒区駒場四丁目6番1号
【氏名又は名称】	財団法人生産技術研究奨励会

【代理人】

申請人

【識別番号】	100064908
--------	-----------

【住所又は居所】	東京都中央区八重洲2丁目3番1号 志賀国際特許事務所
----------	----------------------------

【氏名又は名称】	志賀 正武
----------	-------

【選任した代理人】

【識別番号】	100108578
--------	-----------

【住所又は居所】	東京都中央区八重洲2丁目3番1号 志賀国際特許事務所
----------	----------------------------

【氏名又は名称】	高橋 詔男
----------	-------

【選任した代理人】

【識別番号】	100089037
--------	-----------

【住所又は居所】	東京都中央区八重洲2丁目3番1号 志賀国際特許事務所
----------	----------------------------

【氏名又は名称】	渡邊 隆
----------	------

【選任した代理人】

【識別番号】	100101465
--------	-----------

【住所又は居所】	東京都中央区八重洲2丁目3番1号 志賀国際特許事務所
----------	----------------------------

【氏名又は名称】	青山 正和
----------	-------

【選任した代理人】

【識別番号】	100094400
--------	-----------

【住所又は居所】	東京都中央区八重洲2丁目3番1号 志賀国際特許事務所
----------	----------------------------

【氏名又は名称】	鈴木 三義
----------	-------

【選任した代理人】

【識別番号】 100107836

【住所又は居所】 東京都中央区八重洲 2 丁目 3 番 1 号 志賀国際特
許事務所

【氏名又は名称】 西 和哉

【選任した代理人】

【識別番号】 100108453

【住所又は居所】 東京都中央区八重洲 2 丁目 3 番 1 号 志賀国際特
許事務所

【氏名又は名称】 村山 靖彦

特願 2 0 0 3 - 3 6 7 5 2 7

出 願 人 履 歴 情 報

識別番号 [8 0 1 0 0 0 0 4 9]

1. 変更新月日	2 0 0 1 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都目黒区駒場四丁目 6 番 1 号
氏 名	財団法人生産技術研究奨励会

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.